The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/2/2014

SUBJECT:

Multiple Vulnerabilities in Mozilla Firefox and Thunderbird Could Allow for Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been identified in Mozilla Firefox and Thunderbird that could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet and Mozilla Thunderbird is an email client. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Mozilla Firefox versions prior to 34
- Mozilla Firefox Extended Support Release (ESR) version prior to 31.3
- Mozilla Thunderbird versions prior to 31.3

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Nine vulnerabilities have been reported in Mozilla Firefox and Thunderbird. Details of the vulnerabilities are as follows:

- Mozilla Firefox and Thunderbird are prone to multiple unspecified memory-corruption vulnerabilities that exist in the browser engine. [CVE-2014-1587, CVE-2014-1588, MFSA 2014-83]
- Mozilla Firefox is prone to an unspecified security-bypass vulnerability when processing specially crafted Chrome based CSS stylesheets that have an improperly declared namespaces. [CVE-2014-1589, MFSA 2014-84]
- Mozilla Firefox and Thunderbird are prone to a denial-of-service vulnerability when passing a JavaScript object to XMLHttpRequest that mimics an input stream. [CVE-2014-1590, MFSA 2014-85]
- Mozilla Firefox is prone to an information-disclosure vulnerability because Content Security Policy leaks redirect data through violation reports. [CVE-2014-1591, MFSA 2014-86]
- Mozilla Firefox and Thunderbird are prone to a use-after-free memory-corruption vulnerability when creating a second root element during the parsing of an HTML5 document that contains 'document.open()'. [CVE-2014-1592, MFSA 2014-87]
- Mozilla Firefox and Thunderbird are prone to a buffer-overflow vulnerability. Specifically, when handling a specially crafted media content. [CVE-2014-1593, MFSA 2014-88]
- Mozilla Firefox and Thunderbird are prone to a security vulnerability which occurs due to a bad casting from the BasicThebesLayer to BasicContainerLayer. [CVE-2014-1594, MFSA 2014-89]
- Mozilla Firefox and Thunderbird are prone to multiple information-disclosure vulnerabilities because the CoreGraphics framework of OS X stores all the Mozilla input into a log file located in the '/tmp' local directory. [CVE-2014-1595, MFSA 2014-90]

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Mozilla to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Mozilla:

https://www.mozilla.org/security/announce/2014/mfsa2014-83.html

https://www.mozilla.org/security/announce/2014/mfsa2014-84.html

https://www.mozilla.org/security/announce/2014/mfsa2014-85.html

https://www.mozilla.org/security/announce/2014/mfsa2014-86.html

https://www.mozilla.org/security/announce/2014/mfsa2014-87.html

https://www.mozilla.org/security/announce/2014/mfsa2014-88.html

https://www.mozilla.org/security/announce/2014/mfsa2014-89.html

https://www.mozilla.org/security/announce/2014/mfsa2014-90.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1587

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1588

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1589

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1590

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1591

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1592

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1593

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1594

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1595

Security Focus:

http://www.securityfocus.com/bid/71391

http://www.securityfocus.com/bid/71392

http://www.securityfocus.com/bid/71393

http://www.securityfocus.com/bid/71394

http://www.securityfocus.com/bid/71395

http://www.securityfocus.com/bid/71396

http://www.securityfocus.com/bid/71397

http://www.securityfocus.com/bid/71398

http://www.securityfocus.com/bid/71399